IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

WIKIMEDIA FOUNDATION, *Plaintiff*, v. NATIONAL SECURITY AGENCY / CENTRAL SECURITY SERVICE, *et al.*, *Defendants*.	Hon. T.S. Ellis, III Civil Action No. 15-cv-00662-TSE

PLAINTIFF WIKIMEDIA FOUNDATION'S SUR-REPLY IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

David R. Rocah (Bar No. 27315)
Deborah A. Jeon (Bar No. 06905)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

Benjamin H. Kleine (pro hac vice)
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

Patrick Toomey (pro hac vice)
Ashley Gorski (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Alex Abdo (pro hac vice)
Jameel Jaffer (pro hac vice)
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Counsel for Plaintiff

Table of Contents

Table of Authorities

Cases

Statutes

Rules

Other Authorities

Introduction

In their desire to avoid the merits of this case, Defendants ask the Court to turn the summary judgment standard on its head and to disregard an evidentiary record built on their own unclassified, public disclosures.

In reality, the government has fallen far short of its burden on summary judgment. Wikimedia has standing because it is virtually certain that the NSA is copying and reviewing at least some of Wikimedia's trillions of Internet communications. This conclusion flows from three key facts. First, as the government concedes, Wikimedia's communications traverse every circuit carrying public Internet traffic on every cable connecting the U.S. with the rest of the world. Second, as the government has acknowledged, the NSA monitors communications at one or more of these "international Internet link[s]." Third, as Wikimedia's expert Scott Bradner explains, the NSA could not conduct Upstream surveillance as it has described it without copying and reviewing Wikimedia's communications on each circuit it monitors.

Bradner's conclusion is directly and independently supported by two documents declassified by the government: the FISC opinion of October 3, 2011, and the PCLOB Report on Section 702 surveillance. These documents describe in detail how the NSA has implemented Upstream surveillance and the technological constraints it faces in doing so. Even setting these disclosures aside, additional technical and practical necessities support Bradner's conclusion that the NSA is copying and reviewing some Wikimedia traffic as it scours Internet traffic for communications associated with its targets. Finally, Bradner describes another basis for his conclusion that the NSA is at least *copying* Wikimedia's communications: the fact that the NSA "most likely" uses a copy-then-filter configuration to implement Upstream surveillance. The government characterizes Bradner's use of the phrase "most likely" as a fatal concession, but it simply misunderstands the argument, which is entirely independent of Bradner's other bases for

concluding that the NSA is copying and reviewing Wikimedia's communications.

Tellingly, the government has been unable to find any expert—including Henning Schulzrinne—willing to argue that the NSA is *not* copying and reviewing Wikimedia's communications. Instead, Schulzrinne poses a series of hypotheticals about what the NSA could do if it wanted to design an Internet surveillance system that avoided Wikimedia's traffic. But in the end, Schulzrinne's Wikimedia-avoidance theory is just that: a theory. The government offers no evidence that the NSA is, in fact, doing any of these things. And even Schulzrinne refuses to assign his own opinions any weight in the real world. The Court should do the same.

Recognizing this weakness, the government seeks to have Bradner's declaration cast out as inadmissible, arguing that an expert technologist is not permitted to describe the technical implications of, or to make reasoned inferences based on, the government's many disclosures about Upstream surveillance. But because Bradner plainly applies his specialized knowledge to this factual record, his expert opinion is admissible under *Daubert*.

Finally, the state secrets privilege does not apply here, much less justify dismissal. Given the extensive public record concerning Upstream surveillance, it is plain that this case can and should proceed—using the procedures Congress established in FISA, which obligate courts to examine FISA materials in camera to resolve civil challenges like this one. 50 U.S.C. § 1806(f).

I. The government distorts the applicable legal standards.

To prevail, the government must establish that there is no genuine dispute as to whether Wikimedia faces a substantial risk that *any* of its Internet communications will be copied or reviewed under Upstream surveillance. Contrary to the government's claims, recent and controlling precedent is clear that a plaintiff seeking prospective relief may establish standing by demonstrating a "substantial risk" of harm. *See Susan B. Anthony List v. Driehaus*, 573 U.S. 149,

157-58 (2014); *Beck v. McDonald*, 848 F.3d 262, 275 (4th Cir. 2017).[1] In any event, whether this Court applies the "substantial risk" standard or the "certainly impending" standard, the government has failed to establish that there is no dispute of material fact.

Faced with Wikimedia's evidence, the government seeks to prevail by flipping the summary judgment burden. It wrongly contends that Wikimedia can survive summary judgment only if it disproves each of Schulzrinne's theoretical possibilities and establishes with perfect certainty that the NSA "must be" copying and reviewing its communications. But that is not Wikimedia's burden. The question here is whether Wikimedia has presented evidence that its communications are at substantial risk of being copied and reviewed by the NSA. Wikimedia has presented evidence of that injury and others.

II. Because Wikimedia has presented admissible evidence of its standing, the government's motion for summary judgment fails.

Wikimedia has demonstrated its standing by presenting admissible evidence that (1) its communications traverse every international Internet link carrying public Internet traffic into and out of the U.S., (2) the NSA conducts Upstream surveillance on at least one such link, and (3) the NSA could not conduct Upstream surveillance as it has described it without copying and reviewing Wikimedia's communications on each link it monitors. 2d Bradner Decl. ¶¶ 17-60.

Defendants are mistaken in arguing that Wikimedia no longer maintains that its communications "must be" copied and reviewed in the course of Upstream surveillance. Although that is not Wikimedia's burden to prove here, that is what the evidence shows. Based on the government's own documents, Bradner explains why the NSA could not conduct the surveillance it has publicly described without copying, reassembling, and reviewing *all* the

[1] The government claims its cases impose a further "actual action" requirement, but none of them do. *See* Def. Reply 3-4. Even if that were required, the relevant action here would be the NSA's use of Upstream surveillance to monitor Internet traffic flowing in and out of the U.S.

international communications on the circuits it is monitoring. 2d Bradner Decl. ¶¶ 27-54. But even if one ignores these key disclosures—as Schulzrinne does when he theorizes about filtering—Bradner explains why it is still a virtual certainty that the NSA is copying and reviewing at least some of *Wikimedia's* communications. *Id.* ¶¶ 55-155.

By contrast, Schulzrinne provides no evidence that the NSA has *ever* pursued his Wikimedia-avoidance theory. The Court could credit his opinion only if it drew inference upon inference in his favor—the opposite of what it must do at summary judgment. At most, Schulzrinne's critiques of Bradner's opinions confirm that summary judgment should be denied.

A. The NSA is copying and reviewing some of Wikimedia's trillions of communications as they transit international Internet links.

1. It is undisputed that Wikimedia's communications traverse every circuit carrying public Internet traffic on every cable connecting the U.S. with the rest of the world.

Wikimedia's evidence on this point is undisputed. Def. Br. 1-2 (ECF No. 166).

2. The NSA has admitted that it conducts Upstream surveillance on at least one international Internet link.

As the FISC explained, the NSA has conceded that it conducts Upstream surveillance on at least one "international Internet link," [*Redacted*], 2011 WL 10945618, at *15 (FISC Oct. 3, 2011), which is a link between the United States and a foreign country, Bradner Decl. ¶ 225. Defendants argue that the FISC's statement is inadmissible hearsay. Def. Reply 5. This claim is remarkable given that Defendants declassified and released the FISC opinion, but it is also a distraction. The NSA admitted at its 30(b)(6) deposition that the FISC's statement was "accurate." Richards Depo. 159:21-160:17 (ECF No. 143-3); *see* Fed. R. Evid. 801(2)(B).[2]

The facts in the FISC opinion are admissible in their entirety for additional reasons: (1)

[2] Although the FISC issued this opinion in 2011, it is plainly probative evidence of how Upstream surveillance has been conducted since then. Fed. R. Evid. 401.

the NSA adopted those facts at its deposition, *see* Richards Depo. 173:22-175:8; (2) the government is estopped from denying those facts because it was a party to the underlying proceedings and because the question of how Upstream surveillance operates was litigated to a final judgment, *see McHan v. Comm'r*, 558 F.3d 326, 331 (4th Cir. 2009); and (3) the FISC conducted an exhaustive investigation and, unlike in *Nipper v. Snipes*, 7 F.3d 415, 418 (4th Cir. 1993), there is no risk of prejudice from admitting the opinion. *See* Fed. R. Evid. 803(8), 807.[3]

3. The government's official disclosures show that the NSA is copying and reviewing some of Wikimedia's communications.

Wikimedia's expert, Scott Bradner, provides three independent bases for his conclusion that, for technical reasons, the NSA must be copying and reviewing Wikimedia's communications as they traverse international Internet links monitored by the NSA: (1) the FISC's technical explanation that the NSA "will acquire" certain Internet communications traversing the international Internet links it is monitoring, *see* 2d Bradner Decl. ¶¶ 33-45; (2) the NSA's stated goal of "comprehensively" acquiring communications to or from its targets, *see id*. ¶¶ 46-54; and (3) numerous other technical and practical necessities that make clear the NSA is copying, reassembling, and reviewing Wikimedia's communications, *see id.* ¶¶ 55-60.

First, the technical descriptions in the government's own disclosures show that the NSA is copying and reviewing all communications on the international circuits it monitors. As the government conceded to the FISC, the NSA "*will acquire* a wholly domestic 'about' communication if the transaction containing the communication is routed through an international Internet link being monitored by NSA." [*Redacted*], 2011 WL 10945618, at *15 (emphasis added). This statement reveals a key technological fact about Upstream surveillance at international Internet links. The government's concession could be true only if the NSA were *not*

[3] Even if the FISC opinion were hearsay, Bradner is entitled to rely on it. Fed. R. Evid. 703.

using any kind of filter—whether a whitelist or blacklist—at the international links it is monitoring. Bradner Decl. ¶¶ 293-94; 2d Bradner Decl. ¶¶ 6-8, 25(e), 35-45. Both the government and Schulzrinne try to sidestep this concession, claiming that when the FISC said "will acquire" it really meant "might" or "could" acquire.[4] As a technical matter, however, those are very different things. *Id.* ¶¶ 36, 42-44. Moreover, it is clear that the FISC meant what it said, given that the opinion described the court's exacting investigation into a series of government misrepresentations; that the FISC used the same phrasing elsewhere in its 81-page, highly technical opinion, to describe the same phenomenon; and that it used slightly different phrasing elsewhere to describe a slightly different phenomenon. *Compare* [*Redacted*], 2011 WL 10945618, at *11 ("NSA's upstream collection devices *will acquire* a wholly domestic 'about' SCT if it is routed internationally" (emphasis added)), *with id.* at *11 n.34 (noting that, given technical limitations in a particular context, the "NSA *may* acquire wholly domestic communications" (emphasis added)). These statements contradict Schulzrinne's hypothesized filtering. 2d Bradner Decl. ¶¶ 42-44.

Second, the PCLOB has stated, as part of an exhaustive study, that the NSA's goal is to "comprehensively acquire communications that are sent to or from its targets." PCLOB Report 10, 123, 143 (ECF No. 168-19). The technical reality is that the NSA could not be comprehensive on any particular circuit it is monitoring if it used blacklisting or whitelisting of the sort Schulzrinne hypothesizes. 2d Bradner Decl. ¶¶ 46-44, 63-112. For example, blacklisting IP addresses or protocols would deliberately ignore a target's communications with one of those

[4] For example, Schulzrinne claims that the government's concession is compatible with his hypotheses by arguing that, even if the NSA were whitelisting or blacklisting communications at Internet links, certain wholly domestic communications "*could* still be copied and scanned by the NSA." 2d Schulzrinne Decl. ¶ 58 (emphasis added). But saying that those communications *could* be acquired is not the same as saying that they "*will*" be acquired.

IP addresses or over those protocols, and whitelisting IP addresses or protocols would require the NSA to perform the impossible task of predicting which IP addresses and protocols its thousands of targets will be using at all times. *Id*. ¶¶ 51-53, 68-70, 78-83. Moreover, under "about" collection, the NSA acquired *non-targets'* communications about a target, but it is not possible for the NSA to know in advance which non-targets will be discussing one of its targets. *Id*. ¶¶ 69-70. In short, Schulzrinne's hypotheticals would work only if the NSA were capable of "precognition." *Id*. ¶ 69. To avoid this obvious problem, Defendants claim that the PCLOB did not actually mean "comprehensive" or anything close to it. In other words, Defendants ask the Court to disregard a description of Upstream surveillance contained in an official report of the PCLOB, prepared with extensive input from the NSA, subjected to declassification review by the NSA, and publicly presented as the "exhaustive" unclassified account of Section 702 surveillance. *See* Richards Depo. 144:7-145:12. Moreover, the PCLOB discussed comprehensiveness specifically to explain the *technological* constraints the NSA faces:

> [T]he NSA's acquisition of "about" communications is, to a large degree, an inevitable byproduct of its efforts to comprehensively acquire communications that are to or from its targets. *Because of the specific manner in which the NSA conducts upstream collection, and the limits of its current technology*, the NSA cannot completely eliminate "about" communications from its collection without also eliminating a significant portion of the "to/from" communications it seeks.

PCLOB Report 123 (emphasis added); 2d Bradner Decl. ¶ 48.[5]

The third basis that Bradner describes—and the one Schulzrinne primarily attacks—is the set of other technical and practical necessities that make clear that the NSA is copying, reassembling, and reviewing Wikimedia's communications. *Id*. ¶¶ 55-58. Because the NSA cannot know in advance which packets on a circuit belong to communications that contain

[5] Unlike the plaintiffs in *Klayman v. Obama*, 800 F.3d 559, 563 (D.C. Cir. 2015), Wikimedia has pointed to direct evidence of comprehensiveness.

selectors, it must copy, reassemble, and review all packets belonging to communications of possible interest. *Id.* ¶ 55. As Bradner explains, "[t]he only way that the upstream collection program could possibly avoid all of Wikimedia's ubiquitous communications is if the NSA had actively strived to eliminate them." *Id.* ¶¶ 57, 6. Schulzrinne does not dispute Bradner's technical point but argues that the NSA "in theory could be" attempting to avoid all of Wikimedia's communications. 2d Schulzrinne Decl. ¶¶ 2, 12-13. Schulzrinne concedes that he has "no knowledge" or evidence that the NSA is actually taking any of these steps. Schulzrinne Decl. ¶ 53. Bradner explains at length, however, why Schulzrinne's thought experiment has no traction in the real world, for both technical and practical reasons:

1. Bradner explains why Schulzrinne's hypothetical filtering techniques are directly at odds with the NSA's disclosures. 2d Bradner Decl. ¶¶ 7-8, 33-54, 130-31, 137-38.
2. Bradner explains why, even setting those disclosures aside, it is implausible that the NSA is deliberately ignoring all web communications or all Wikimedia communications using Schulzrinne's techniques. *Id.* ¶¶ 6, 55-59, 61-112, 132-48, 154-55.
3. Bradner explains why the kinds of filtering Schulzrinne hypothesizes would not, in fact, be effective at eliminating all Wikimedia communications. *Id.* ¶¶ 57, 97-101, 140-49.

Finally, Defendants latch onto Bradner's explanation that the NSA is "most likely" using a copy-then-filter method, suggesting that this is a radical concession, Def. Reply 6, but they miss the point. Bradner was laying out an *independent* reason to conclude that Wikimedia's communications are being copied. 2d Bradner Decl. ¶¶ 114-29. He explained that the "most likely" physical configuration of Upstream surveillance equipment makes all of Schulzrinne's filtering theories irrelevant for standing purposes. That is because with the copy-then-filter configuration, any filtering occurs only after the NSA has already copied *all* the communications on a circuit—including Wikimedia's. *Id*. ¶ 114. Even if the NSA used a different configuration, each of the three grounds described above independently support Bradner's conclusion that it is virtually certain that the NSA is copying and reviewing Wikimedia's communications. *Id.* ¶ 115.

B. Bradner's declarations are admissible.

Rule 702 provides that an expert may testify "[i]f scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue." Moreover, "an expert is permitted wide latitude to offer opinions, including those that are not based on firsthand knowledge or observation." *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 592 (1993). Bradner's opinions clearly meet this standard. They are based on his technical expertise, drawn from decades of experience designing and implementing communications networks at Harvard University. Relying on declassified information about the NSA's surveillance activities, Bradner has applied his expertise in Internet technology to reach a set of conclusions about the NSA's implementation of Upstream surveillance.

Defendants argue that Bradner relies on considerations relating to NSA "resources" and "priorities" that are unknown to him, Def. Reply 7, 16, but Defendants ignore the vast majority of the evidence that Bradner relies on to support his central conclusions. Bradner Decl. ¶ 6. Indeed, Bradner's conclusions are plainly based on "good grounds" and "sufficient facts": the government's own detailed descriptions of Upstream surveillance. These include the NSA's submissions to the FISC, the FISC's opinions, the PCLOB Report, the NSA's targeting and minimization procedures, Defendants' discovery responses, the NSA's deposition testimony, and the NSA's public statements. *See* Bradner Decl., App'x List. Bradner's conclusions are corroborated by GCHQ's description of its analogous surveillance program. *See* Bradner Decl. ¶¶ 368-69; 2d Bradner Decl. ¶¶ 140-48. As Defendants admit, Bradner is qualified to opine on the meaning of these documents, the technical requirements necessary to carry out Upstream surveillance as it has been described, and the technical and practical consequences of selecting a particular implementation. All of these matters are well within his specialized knowledge.

Nonetheless, Defendants cherry-pick some of Bradner's criticisms of Schulzrinne's

theory, arguing that Bradner's opinions should be thrown out because he does not have direct or complete knowledge of the NSA's practices. The government is wrong in at least three ways.

First, experts are plainly allowed to provide opinions, make inferences, and weigh probabilities based on their specialized expertise, so long as those opinions and inferences flow from a "sufficient" factual basis. Fed. R. Evid. 702(b). "Sufficient," in this context, does not mean that the expert must have firsthand knowledge of every potentially relevant fact, nor does it mean that the underlying facts must be undisputed. Fed. R. Evid. 702 Advisory Comm. Note.[6]

Second, Bradner has a sufficient factual basis for each of the minor premises that Defendants contest. For example, Defendants claim that Bradner has no basis to suggest that the NSA would be reluctant to disclose any whitelist or blacklist to telecommunications personnel, but Bradner cites his own experience as a technologist working with the government, Bradner Decl. ¶ 286, as well as Defendants' own statements in this case explaining their reluctance to disclose their filtering criteria, 2d Bradner Decl. ¶¶ 106-07. Defendants claim that Bradner has no basis to suggest that the NSA is interested in encrypted communications, but the NSA's own minimization procedures disclose such an interest, Bradner Decl. ¶ 325, and the PCLOB's report makes clear the NSA in fact attempts to decrypt communications acquired under Section 702, PCLOB Report 60, 63. Defendants claim that Bradner has no basis to assume that the NSA has an interest in HTTP or HTTPS communications, but the NSA has disclosed that it collects "web activity." 2d Bradner Decl. ¶¶ 130-31. And Defendants make the bizarre claim that Bradner is

[6] Defendants' cases bear no resemblance to this one because the witnesses in those cases either had no factual basis whatsoever to support their conclusions or admitted they had no specialized expertise in the relevant subject matter. *See* Def. Reply 16 n.11 (citing *Zellers v. NexTech N.E., LLC*, 533 F. App'x 192, 197-98 (4th Cir. 2013) (neurologist who sought to opine on refrigerant toxicology admitted that she was not trained in toxicology and relied on survey of Internet articles); *Oglesby v. GMC*, 190 F.3d 244, 250 (4th Cir. 1999) (witness "did not know the type or composition of the plastic . . . did not ask the manufacturer . . . did not analyze the part"); *Free v. Bondo-Mar-Hyde Corp.*, 25 F. App'x 170, 172 (4th Cir. 2002) (similar)).

speculating when he says that some of the NSA's surveillance targets are "individuals," even though the government has acknowledged this unsurprising fact publicly. 2d Bradner Decl. ¶ 86.[7]

Critically, it is not "speculation" to make a reasoned inference in the absence of direct knowledge. *Daubert*, 509 U.S. at 592. Indeed, when making inferences or reaching conclusions, Bradner is quite careful to tell the Court the level of certainty or confidence he has in his opinion. Defendants treat that honesty as a liability, but it is Schulzrinne who does the Court a disservice by engaging in conjecture while refusing to state whether he believes that, based on the public facts, the NSA is avoiding every one of Wikimedia's trillions of communications.

Finally, at most, Defendants' efforts to cast these various facts into doubt goes to the weight of the evidence at trial—not to the admissibility of Bradner's opinions. *Bresler v. Wilmington Tr. Co.*, 855 F.3d 178, 195 (4th Cir. 2017) ("questions regarding the factual underpinnings of the [expert witness'] opinion affect the weight and credibility of the witness' assessment, not its admissibility"); *M-Edge Accessories LLC v. Amazon.com Inc.*, 2015 WL 403164, at *16 (D. Md. Jan. 29, 2015) (same); *McLean v. 988011 Ontario, Ltd.*, 224 F.3d 797, 806 (6th Cir. 2000) (court erred by excluding expert testimony that was "sufficiently rooted in the available evidence to make out a reasonable theory of causation").

The NSA relies on technology to accomplish its objectives in the real world. 2d Bradner Decl. ¶¶ 10-11. Yet Defendants advance an argument that would insulate the NSA from the informed opinions of outside experts. That argument should be rejected.

[7] Bradner himself addresses each of Defendants' criticisms at greater length. *See, e.g.*, 2d Bradner Decl. ¶¶ 126-29 (disclosure of filters), ¶¶ 116-29 (benefits of copy-then-filter), ¶¶ 125-29 (NSA-operated devices), ¶¶ 80-88 (number of IP addresses), ¶¶ 103-07, 130-36 (blacklisting HTTP/S would leave "blind spots" and a "very large hole"), ¶¶ 137-39 (encrypted communications), ¶¶ 57, 94-96, 132-39 (web and Wikimedia communications), ¶¶ 75-76 (many Upstream targets), ¶¶ 51-52, 69-70, 77-88 (impossible to know targets' IP addresses in advance).

C. Schulzrinne's declarations should be excluded.

The Schulzrinne declarations should be excluded because they consist of a series of hypotheticals. *See* Pl. Opp. 21 & n.8. Schulzrinne offers no opinion on whether Wikimedia's communications are being copied and reviewed by the NSA. He even refuses to offer any opinion on whether the NSA is likely to use any of the whitelisting or blacklisting techniques he hypothesizes, let alone a combination of techniques that might avoid *all* of Wikimedia's communications. Schulzrinne Decl. ¶ 53. As a result, Schulzrinne gives the Court no reliable way of applying his theories to the factual question here. *See Mathias v. Michael Eaves Shoemaker*, 2017 WL 3592457, at *3 (D. Md. Aug. 21, 2017) ("[W]here an expert merely opines as to possibilities and does not opine as to facts, the expert 'is engaging in speculation and conjecture . . . [which] would not assist the trier of fact to understand the evidence in this case or to determine facts in issue.'"); *Nease v. Ford Motor Co.*, 848 F.3d 219, 232 (4th Cir. 2017); *Fedorczyk v. Caribbean Cruise Lines, Ltd.*, 82 F.3d 69, 75 (3d Cir. 1996) ("The possibility of the existence of an event does not tend to prove its probability."). To the extent Schulzrinne ventures beyond hypotheticals, it is only to dispute some of the premises of Bradner's opinion. Thus, at most, Schulzrinne's disputes with Bradner confirm that summary judgment should be denied.

D. Wikimedia has presented admissible evidence of additional injuries that are traceable to Upstream surveillance and independently establish its standing.

Defendants claim that Wikimedia's additional injuries—such as its loss of readership and the measures it has taken to protect its communications—are not traceable to Upstream surveillance, but are instead attributable to "hyperbolic" press reports about NSA activities or mere "subjective fear." *See* Def. Reply 22-27. That argument is wrong factually, because these injuries are traceable to the NSA's own extensive disclosures, *see* Paulson Decl. ¶¶ 40-41, 49-53, but it is also wrong legally. *See Libertarian Party of Va. v. Judd*, 718 F.3d 308, 316 (4th Cir.

2013) (traceability is satisfied if defendant's conduct is "at least in part responsible for [plaintiff's injury] . . . notwithstanding the presence of another proximate cause"); *Hassan v. City of New York*, 804 F.3d 277, 292-93 (3d Cir. 2015); *Sierra Club v. Dep't of the Interior*, 899 F.3d 260, 284 (4th Cir. 2018) (challenged conduct need not be the sole cause of injury).[8]

The government's additional arguments concerning admissibility are unavailing. *See* Def. Reply 24-26. Penney's declarations are directly relevant because they corroborate the evidence of ongoing chill described in the Paulson, Alexander, and Temple-Wood Declarations, and they rest on a reliable statistical foundation. *See* 2d Penney Decl. Finally, the government's argument concerning the admissibility of the NSA slides misunderstands their significance. Def. Reply 23-24. Bradner does not cite or rely on the slides in reaching his conclusions. Rather, the publication of the NSA slides—in addition to the government's disclosures—is evidence of what motivated Wikimedia to implement the protective measures it describes. *See Curtis Lumber Co. v. La. Pac. Corp.*, 618 F.3d 762, 783 n.18 (8th Cir. 2010); Fed. R. Evid. 801(c)(2).[9]

E. Wikimedia has third-party standing to assert the rights of its users.

Wikimedia has third-party standing to assert the rights of its community members—which include its readers and contributors. Pl. Opp. 27-28 & n.12. Wikimedia has presented evidence establishing not only the existence of these users, Alexander Decl. ¶ 10; 2d Temple-Wood Decl.; 2d Bayer Decl., but the many ways in which it fosters and depends upon a close relationship with them. Pl. Opp. 27-28; 2d Paulson Decl. Because users could not file suit without risking the very online privacy and anonymity that this lawsuit seeks to protect,

[8] To show redressability, *see* Def. Reply 27, a plaintiff "need not show that a favorable decision will relieve his *every* injury," *Larson v. Valente*, 456 U.S. 228, 244 n.15 (1982)—much as an injury may have multiple causes and still be "traceable" to one cause.

[9] Likewise, the Wikimedia declarants' discussions about the reactions among community members are not hearsay, *see* Def. Reply 23, because they are offered to demonstrate Wikimedia's state of mind regarding its community's concerns.

Wikimedia has standing to raise its users' claims. Temple-Wood Decl. ¶¶ 18-28; *Enterline v. Pocono Medical Ctr.*, 751 F. Supp. 2d 782, 784-86 (M.D. Pa. 2008).[10]

III. This case can and should proceed using FISA's in camera review procedures.

A. The Court can consider the public, unclassified evidence of Upstream.

The government argues that certain of its *public* disclosures are "privileged facts now removed from the case," Def. Reply 4-5, but no case supports that extraordinary claim. The government also suggests that the Court cannot make legal determinations based on these public facts, but no harm can come from the Court weighing information that the government itself has made public. *See Wikimedia Found. v. NSA*, 335 F. Supp. 3d 772, 784 (D. Md. 2018).

B. Congress has already determined that state secrets are no bar to this case.

Although Defendants now claim that dismissal is required on state secrets grounds, Congress has balanced the interests at stake and has authorized suits like this one to go forward. FISA's mandatory procedures apply here, and they expressly permit the Court to review any privileged material in camera. *See* 50 U.S.C. § 1806(f).

The government asserts, nonetheless, that the state secrets privilege nullifies the procedures that Congress enacted. *See* Def. Reply 21. This is a radical argument. Not only is it unsupported by the government's cases, but it is directly at odds with the Supreme Court's *Youngstown* framework. *See* Pl. Mot. to Compel 16-19 (ECF No. 125-2). As the Ninth Circuit recently held, Section 1806(f) displaces the state secrets privilege in cases like this one—an "affirmative legal challenge[] to electronic surveillance" under FISA. *Fazaga v. FBI*, 2019 WL 961953, at *21-24 (9th Cir. Feb. 28, 2019) (Section 1806(f) "necessarily overrides" the state secrets privilege). The substantial evidentiary record that Wikimedia has adduced is more than

[10] For First Amendment claims, the standing inquiry is relaxed. *Sec'y of State of Md. v. Joseph H. Munson Co.*, 467 U.S. 947, 956 (1984); *Cooksey v. Futrell*, 721 F.3d 226, 235 (4th Cir. 2013).

enough to establish that it is an "aggrieved person" under Section 1806(f). Pl. Opp. 30 & n.13.

But even if FISA's mandatory procedures did not apply here, the state secrets privilege would not compel dismissal. The government makes no claim that the very subject-matter of this case is a state secret, and it has declassified all of the facts about Upstream surveillance necessary for the Court to hold that Wikimedia has standing.[11] *Compare El-Masri v. United States*, 479 F.3d 296, 308-09 (4th Cir. 2007), *with DTM Research, LLC v. AT&T Corp.*, 245 F.3d 327, 334 (4th Cir. 2001) (privileged evidence not "central"). The parties have already conducted extensive discovery and depositions without disclosure of state secrets, and the government fails to show any new or genuine risk of disclosure that would justify dismissal.

Citing a list of purportedly "privileged facts," the government contends that it is entitled to judgment because it could be "deprived of its defense" at trial. Def. Reply 19-20. But again, FISA's in camera review procedures accommodate this very concern. Even if they did not apply, the government has failed to establish an entitlement to dismissal on this ground. Courts have dismissed suits where state secrets prevent the defendant from raising a *valid* defense, *i.e.*, a legally "meritorious" defense that would "require judgment for the defendant." *In re Sealed Case*, 494 F.3d 139, 149 (D.C. Cir. 2007); *see Fazaga*, 2019 WL 961953, at *40 (requiring in camera review to assess validity of defense). The government has not even attempted to make that showing, and the Court has had no opportunity to examine whether the privileged evidence actually supports any claim that Wikimedia's communications are *not* being copied or reviewed.

Conclusion

For the reasons above, Defendants' motion should be denied.

[11] Contrary to Defendants' claim, the Court's ultimate ruling would not reveal whether Wikimedia "is or was" subject to Upstream surveillance, but only whether—based on the public evidence—the interception of Wikimedia's communications was sufficiently likely to confer standing. *See* Pl. Reply on Mot. to Compel 11 (ECF No. 143).

Dated: March 8, 2018

Respectfully submitted,

/s/ David R. Rocah
David R. Rocah (Bar No. 27315)
Deborah A. Jeon (Bar No. 06905)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND
3600 Clipper Mill Rd., #350
Baltimore, MD 21211
Phone: (410) 889-8555
Fax: (410) 366-7838
rocah@aclu-md.org

/s/ Patrick Toomey
Patrick Toomey (pro hac vice)
(*signed by Patrick Toomey with permission of David R. Rocah*)
Ashley Gorski (pro hac vice)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

Benjamin H. Kleine (pro hac vice)
COOLEY LLP
101 California Street, 5th Floor
San Francisco, CA 94111
Phone: (415) 693-2000
Fax: (415) 693-2222
bkleine@cooley.com

Alex Abdo (pro hac vice)
Jameel Jaffer (pro hac vice)
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, NY 10115
Phone: (646) 745-8500
alex.abdo@knightcolumbia.org

Counsel for Plaintiff